PIX/ASA als een Remote VPN-server met uitgebreide verificatie met behulp van CLI en ASDM-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco 5500 Series adaptieve security applicatie (ASA) moet configureren om op te treden als een externe VPN-server met behulp van Adaptieve Security Devices Manager (ASDM) of CLI. De ASDM levert veiligheidsbeheer en controle van wereldklasse door middel van een intuïtieve, makkelijk te gebruiken web-gebaseerde beheerinterface. Nadat de Cisco ASA-configuratie is voltooid, kan deze worden geverifieerd met behulp van de Cisco VPN-client.

Raadpleeg PIX/ASA 7.x en Cisco VPN-client 4.x met Windows 2003 IAS RADIUS (Against Active Directory) verificatievoorbeeld voor het instellen van de VPN-verbinding op afstand tussen een Cisco VPN-client (4.x voor Windows) en de PIX 500 Series security applicatie 7.x. De externe VPN-clientgebruiker authenticeert de actieve map met een Microsoft Windows 2003-server voor internetverificatie (IAS) RADIUS.

Raadpleeg PIX/ASA 7.x en Cisco VPN-client 4.x voor Cisco Secure ACS-verificatie Configuratievoorbeeld om een VPN-verbinding op afstand in te stellen tussen een Cisco VPN-client (4.x voor Windows) en PIX 500 Series security applicatie 7.x met een Cisco Secure Access Control Server (ACS versie 3.2) voor uitgebreide verificatie (Xauth).

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de ASA volledig operationeel en geconfigureerd is om Cisco ASDM of CLI in staat te stellen configuratiewijzigingen door te voeren.

Opmerking: Raadpleeg HTTPS-toegang voor ASDM of PIX/ASA 7.x: SSH in het Voorbeeld van de configuratie van binnen en buiten om het apparaat extern te kunnen configureren door de ASDM of Secure Shell (SSH).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Software voor Cisco adaptieve security applicatie, versie 7.x en hoger
- Adaptieve Security Office Manager versie 5.x en hoger
- Cisco VPN-clientversie 4.x en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco PIX security applicatie versie 7.x en hoger.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Remote-toegangsconfiguraties bieden beveiligde externe toegang voor Cisco VPN-clients, zoals mobiele gebruikers. Een VPN-toegang op afstand stelt externe gebruikers in staat om veilig toegang te krijgen tot gecentraliseerde netwerkbronnen. De Cisco VPN-client voldoet aan het IPSec-protocol en is specifiek ontworpen om met het security apparaat te werken. Het security apparaat kan echter wel IPSec-verbindingen maken met veel klanten die aan het protocol voldoen. Raadpleeg de ASA Configuration Guides voor meer informatie over IPSec.

Groepen en gebruikers zijn kernconcepten in het beheer van de beveiliging van VPN's en in de configuratie van het security apparaat. Ze specificeren eigenschappen die de toegang van gebruikers tot en het gebruik van VPN bepalen. Een groep is een verzameling gebruikers die als één entiteit worden behandeld. Gebruikers krijgen hun eigenschappen van groepsbeleid. Tunnelgroepen identificeren het groepsbeleid voor specifieke verbindingen. Als u geen bepaald groepsbeleid aan een gebruikers toewijst, is het standaard groepsbeleid voor de verbinding van toepassing.

Een tunnelgroep bestaat uit een reeks records die tunnelverbindingsbeleid bepalen. In deze registers worden de servers geïdentificeerd waarop de servers waarop de tunnelgebruikers zijn geauthentiseerd, evenals de eventuele boekhoudservers waarop de aansluitingsinformatie wordt verzonden. Ze identificeren ook een standaardgroepsbeleid voor de verbindingen, en ze bevatten protocol-specifieke verbindingsparameters. Tunnelgroepen omvatten een klein aantal eigenschappen die betrekking hebben op de totstandbrenging van de tunnel zelf. Tunnelgroepen bevatten een muiswijzer op een groepsbeleid dat gebruikersgeoriënteerde eigenschappen definieert.

Opmerking: In de steekproefconfiguratie in dit document worden lokale gebruikersrekeningen gebruikt voor authenticatie. Als u een andere service wilt gebruiken, zoals LDAP en RADIUS, raadpleegt u Een externe RADIUS-server configureren voor autorisatie en verificatie.

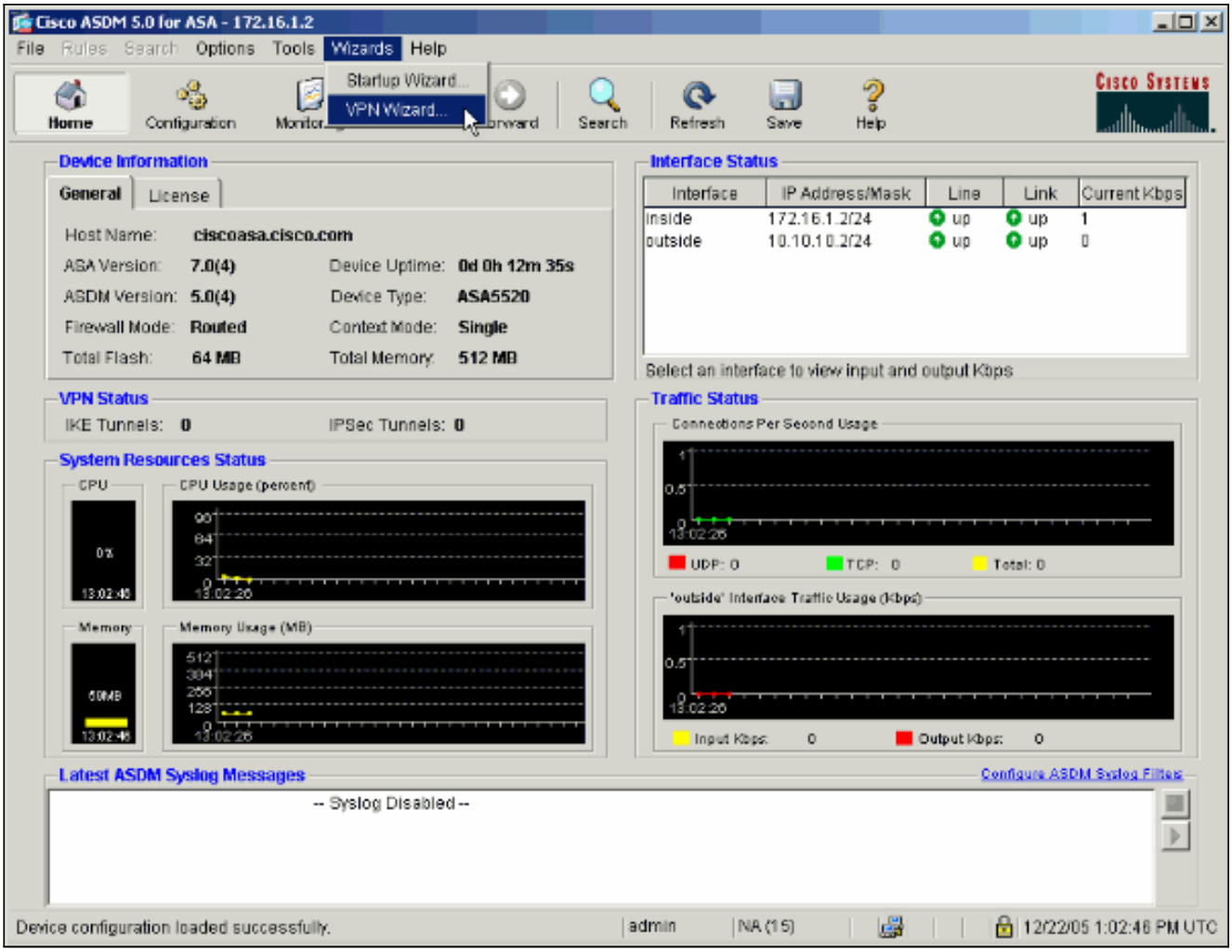
De Internet Security Association en het Key Management Protocol (ISAKMP), ook IKE genoemd, is het onderhandelingsprotocol dat hosts overeenstemming bereikt over de manier waarop een IPSec Security Association moet worden gebouwd. Elke ISAKMP-onderhandeling is verdeeld in twee delen, fase1 en fase2. Fase1 creëert de eerste tunnel om latere ISAKMP-onderhandelingsberichten te beschermen. Phase2 creëert de tunnel die gegevens beschermt die over de veilige verbinding reiken. Raadpleeg ISAKMP-beleidstrefwoorden voor CLI-opdrachten voor meer informatie over ISAKMP.

Configuraties

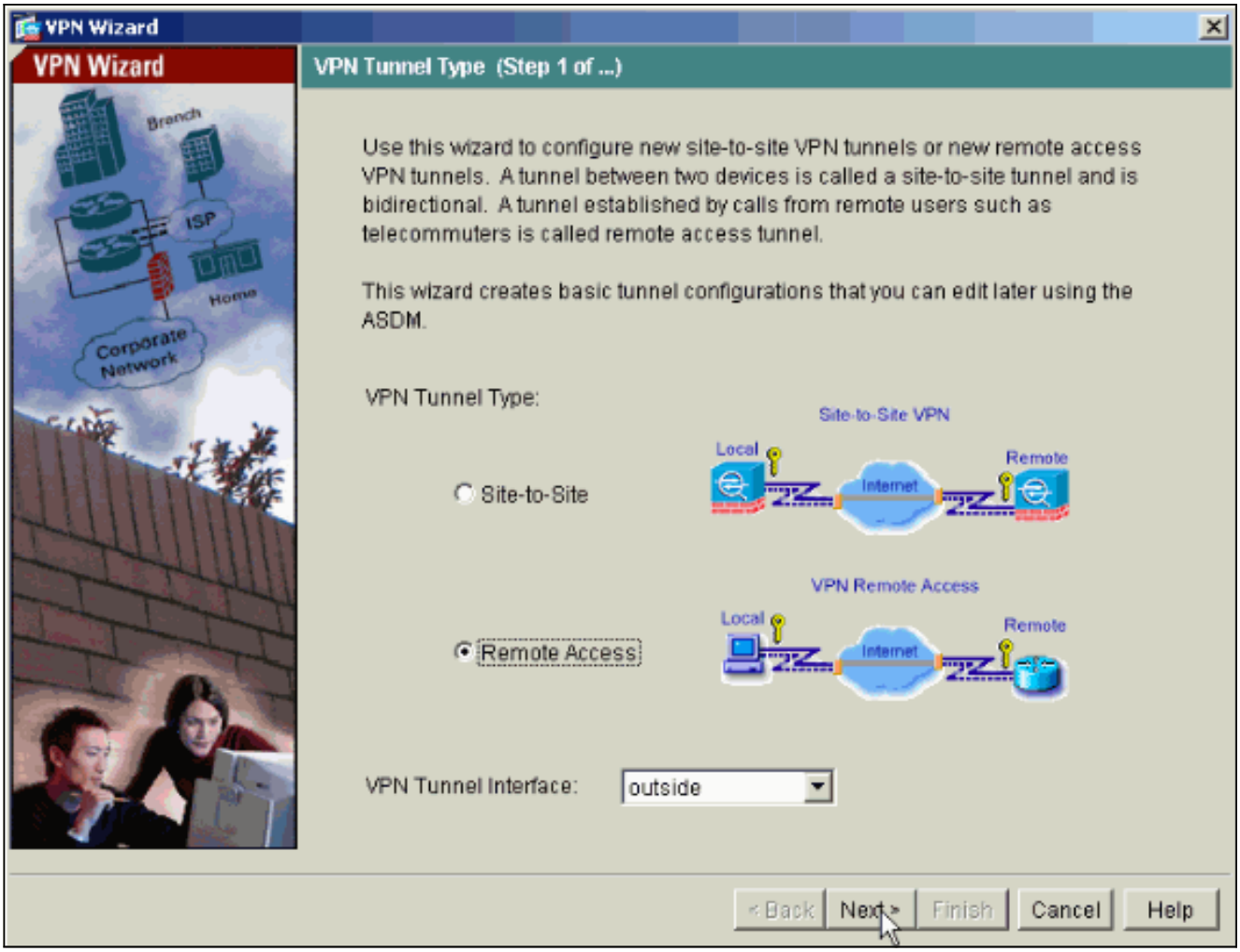
ASA/PIX configureren als een externe VPN-server met ASDM

Voltooi deze stappen om Cisco ASA als een externe VPN-server te configureren met behulp van ASDM:

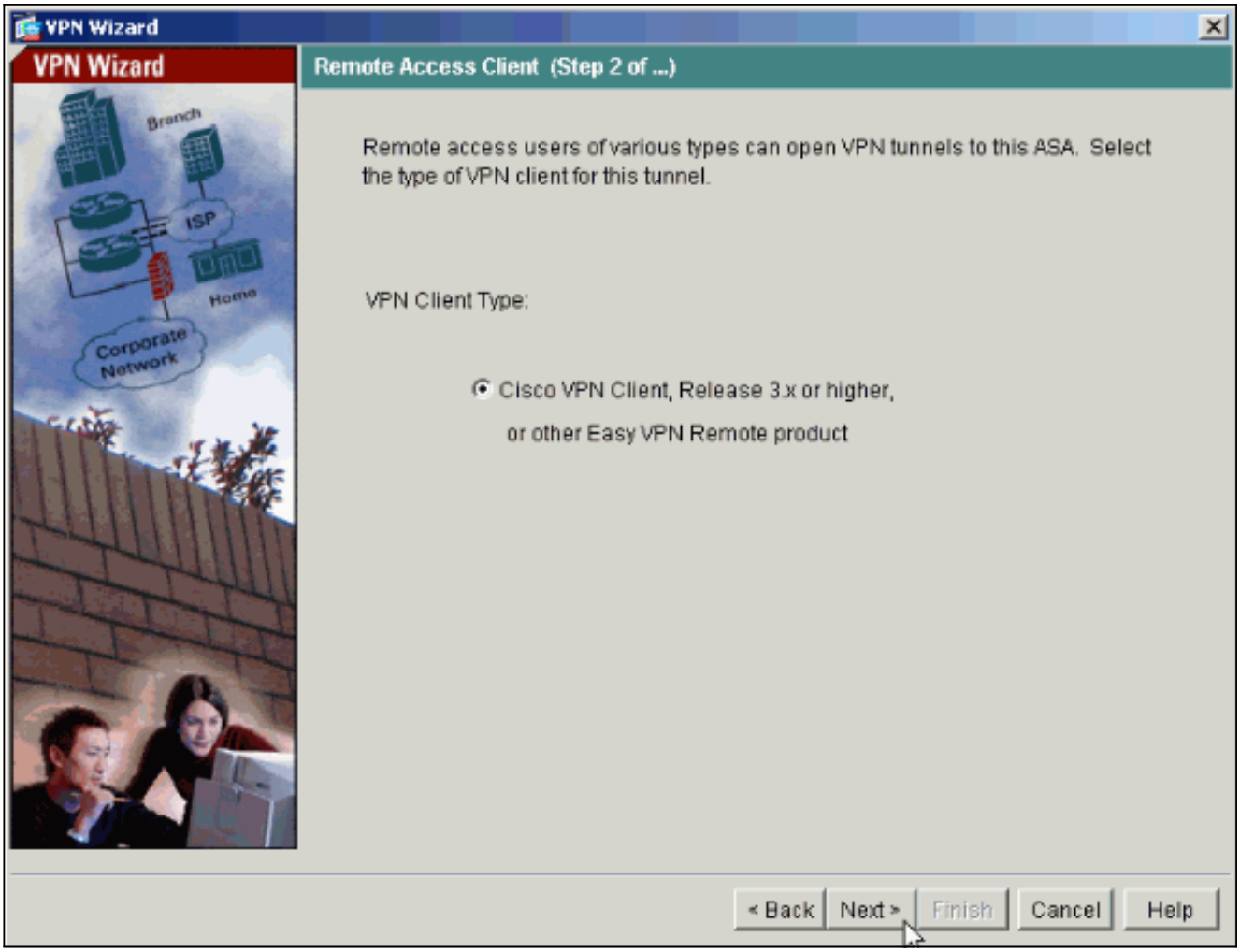
1. Selecteer **Wizard > VPN** vanuit het venster Start.



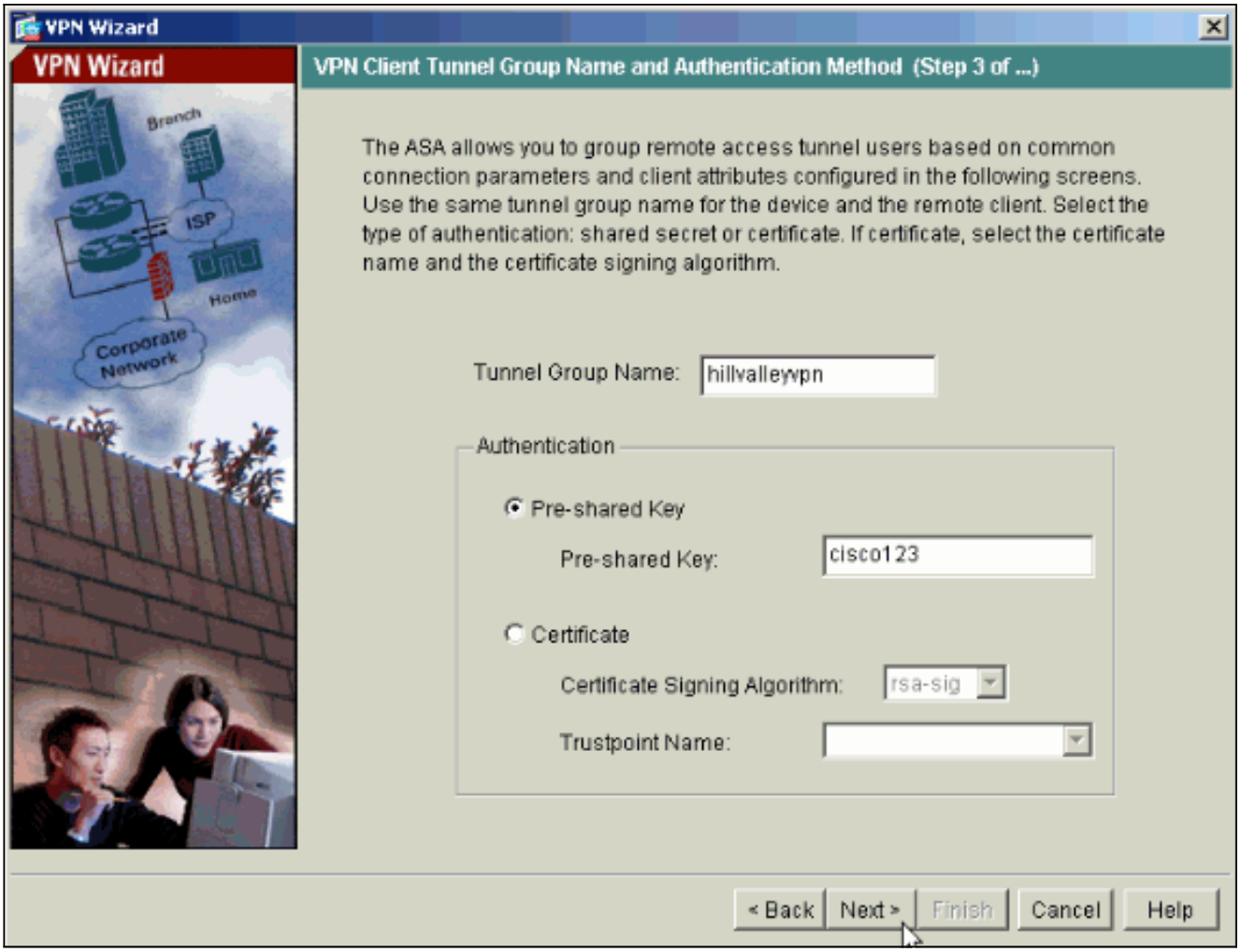
2. Selecteer het tunneltype **Remote Access** VPN en zorg ervoor dat de VPN-tunnelinterface naar wens wordt
ingesteld.



3. Het enige beschikbare VPN-clienttype is al geselecteerd. Klik op **Volgende**.

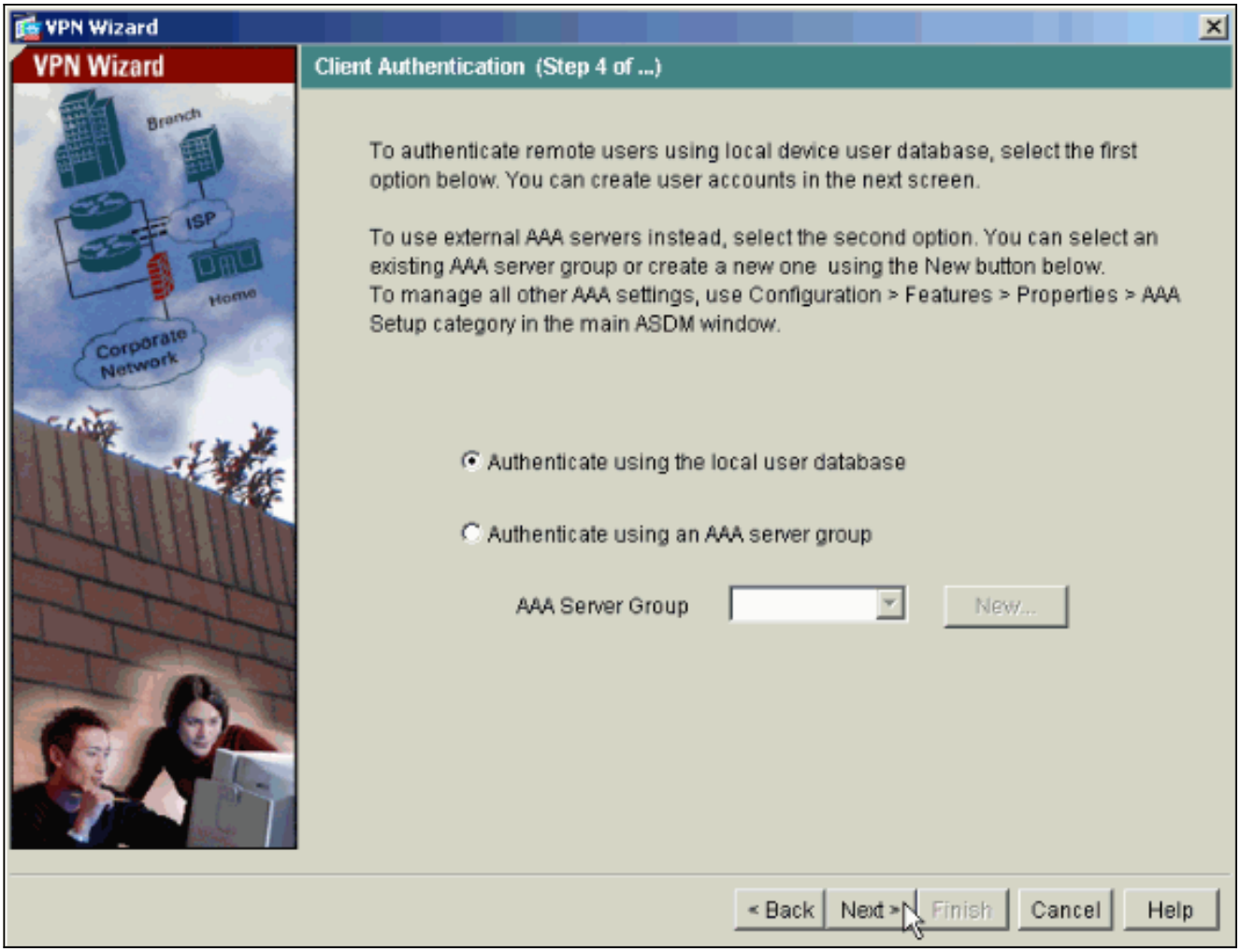


4. Voer een naam in voor de naam van de tunnelgroep. Verstrek de te gebruiken authenticatie informatie.**Vooraf gedeelde sleutel** is geselecteerd in dit voorbeeld.

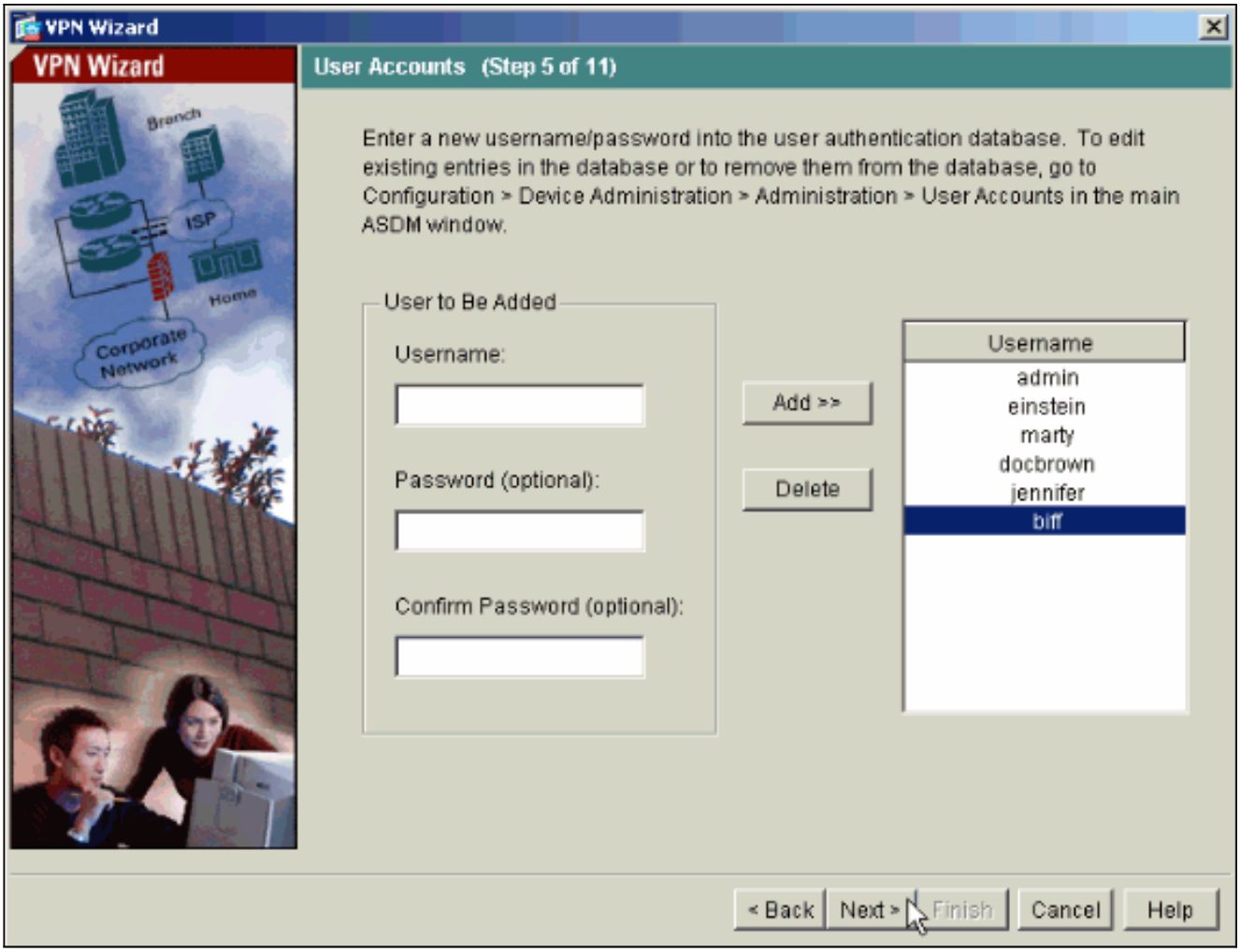


N.B.: Er is geen manier om de voorgedeelde toets op de ASDM te verbergen of te versleutelen. De reden is dat ASDM alleen gebruikt mag worden door mensen die de ASA configureren of door mensen die de klant bijstaan met deze configuratie.

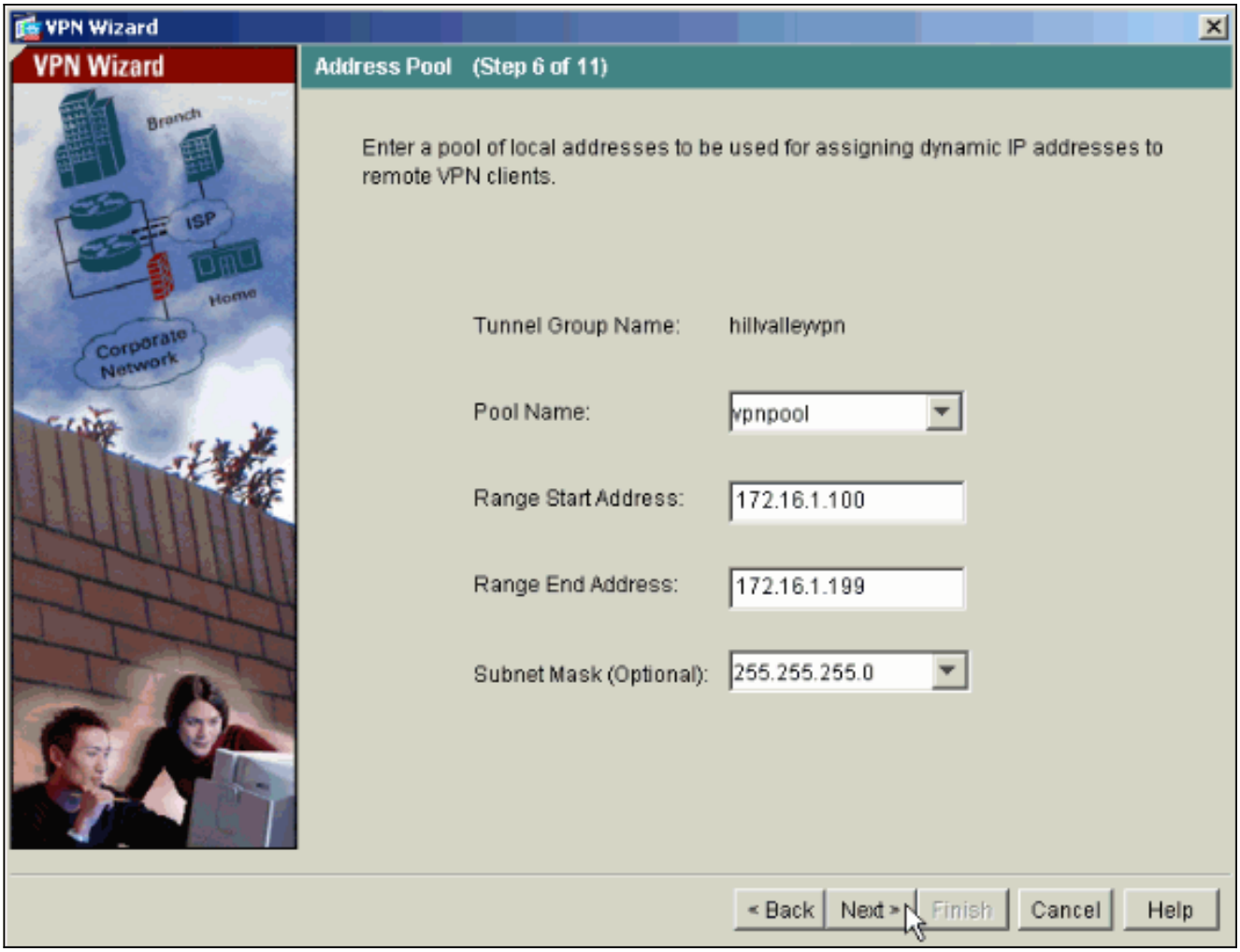
5. Kies of u externe gebruikers wilt geauthentiseerd worden naar de lokale gebruikersdatabase of naar een externe AAA server groep.**Opmerking:** U voegt in stap 6 gebruikers toe aan de lokale gebruikersdatabase.**Opmerking:** Raadpleeg PIX/ASA 7.x-groepen voor VPN-gebruikers via ASDM Configuration Voorbeeld voor informatie over de configuratie van een externe AAA-servergroep via
ASDM.



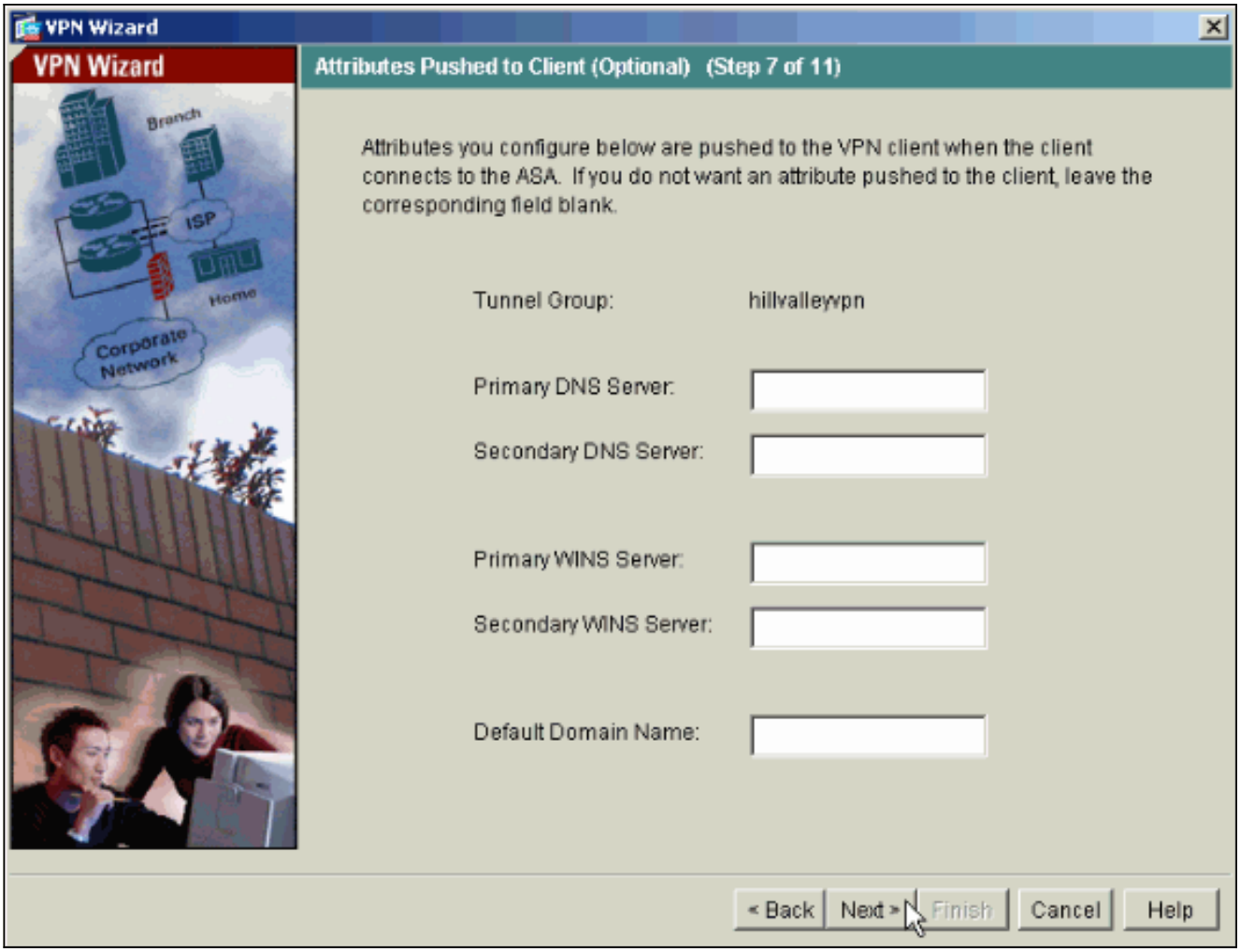
6. Voeg indien nodig gebruikers toe aan de lokale database.**N.B.:** Verwijder bestaande gebruikers niet uit dit venster. Selecteer **Configuratie > Apparaatbeheer > Administratie > Gebruikersrekeningen in het hoofdvenster van ASDM** om bestaande items in de database te bewerken of deze uit de database te verwijderen.



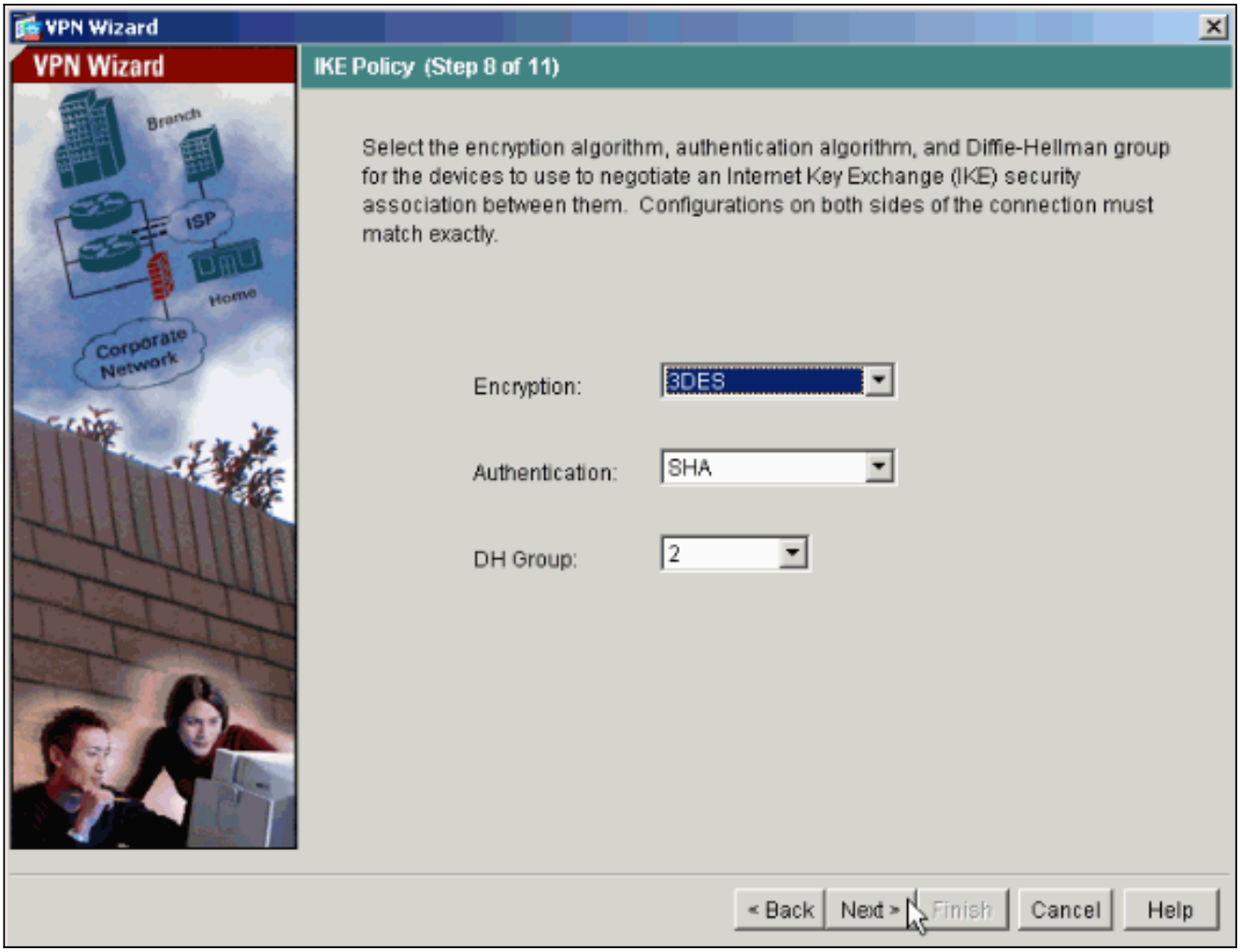
7. Defineert een pool van lokale adressen die dynamisch aan externe VPN-clients moeten worden toegewezen wanneer ze verbinding maken.



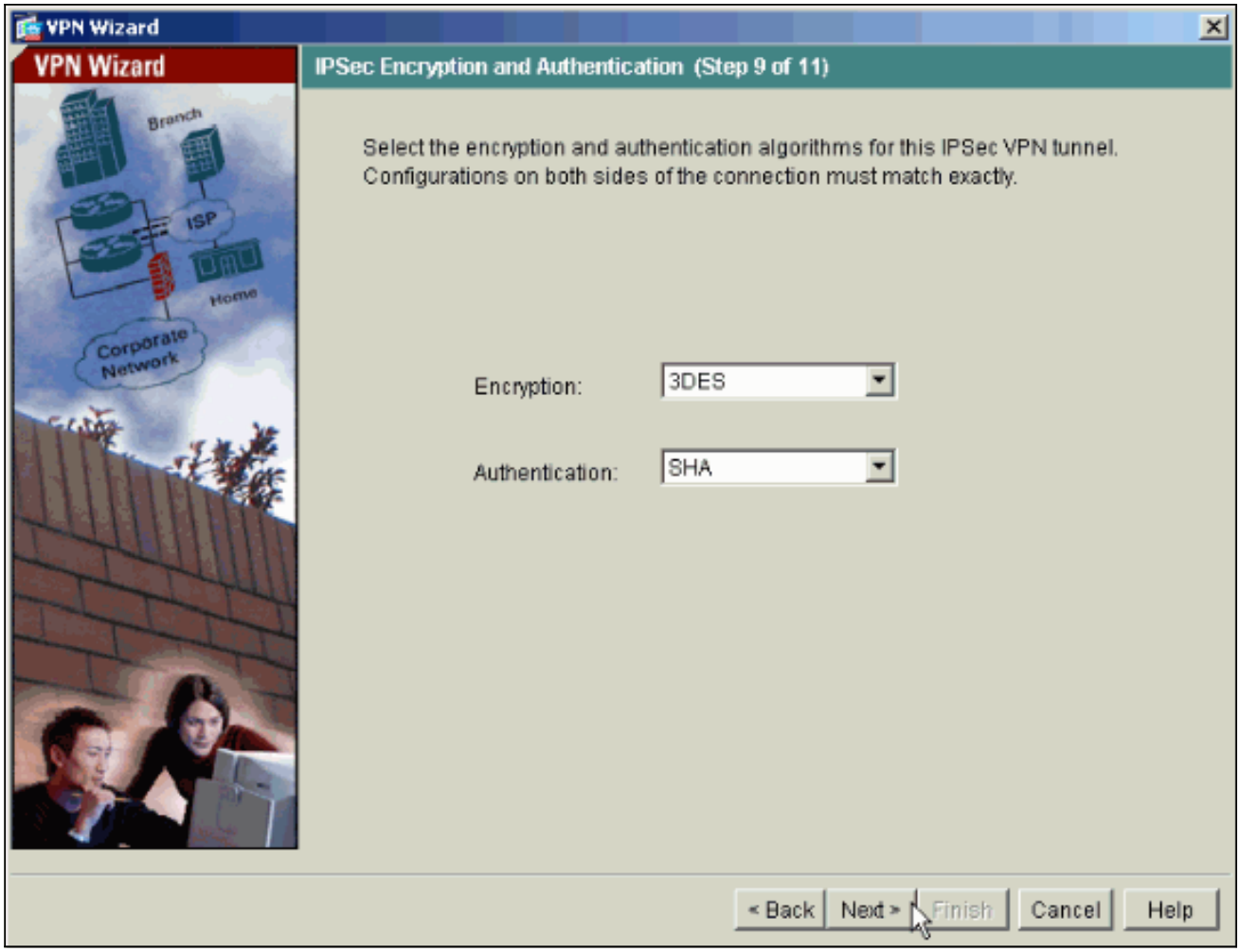
8. *Optioneel:* Specificeer de DNS- en WINS-serverinformatie en een standaardnaam voor domeinen die naar externe VPN-clients moet worden geduwd.



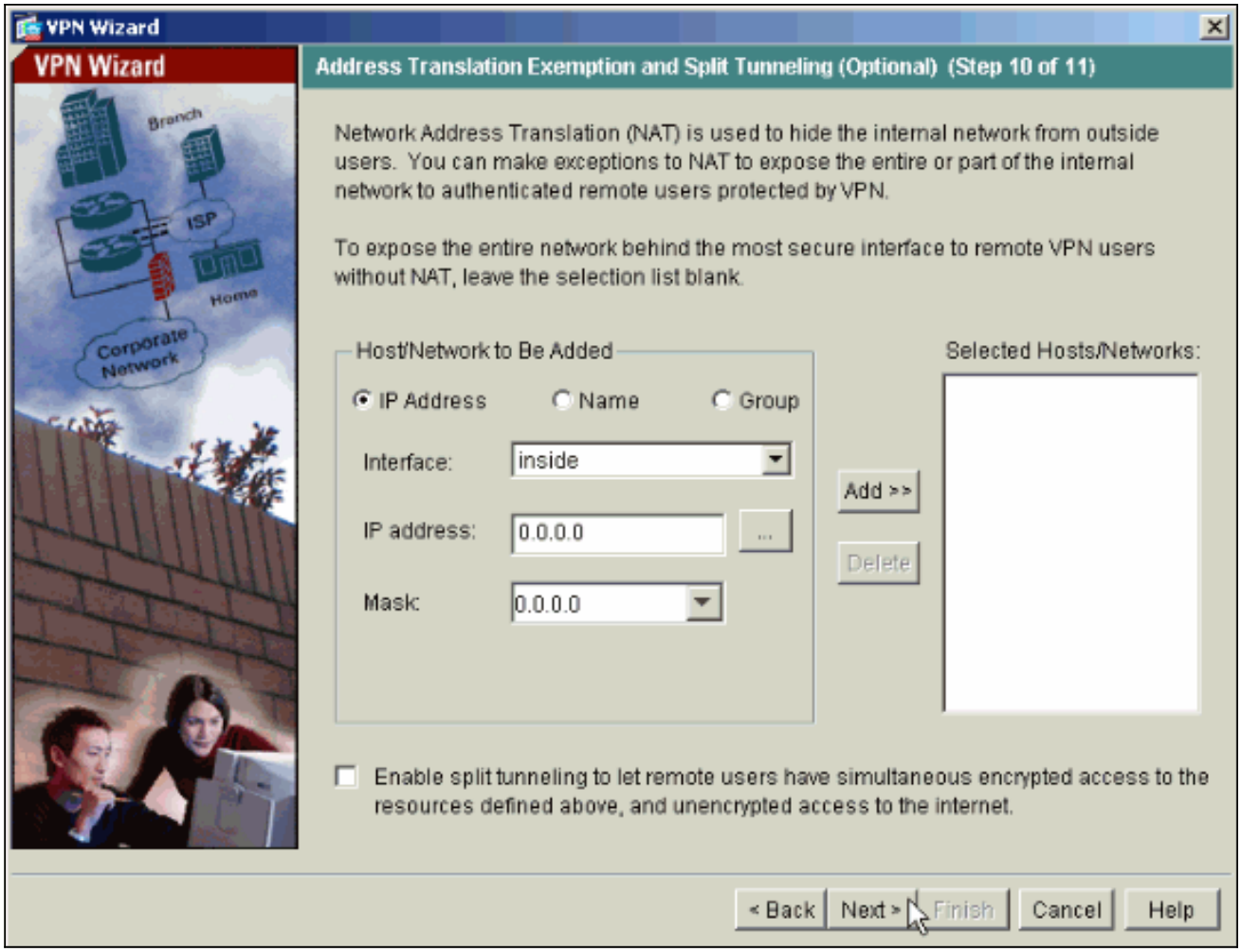
9. Specificeer de parameters voor IKE, ook bekend als IKE Fase 1.De configuraties aan beide zijden van de tunnel moeten precies overeenkomen. Maar de Cisco VPN-client selecteert automatisch de juiste configuratie voor zichzelf. Daarom is geen IKE-configuratie nodig op de client-
pc.



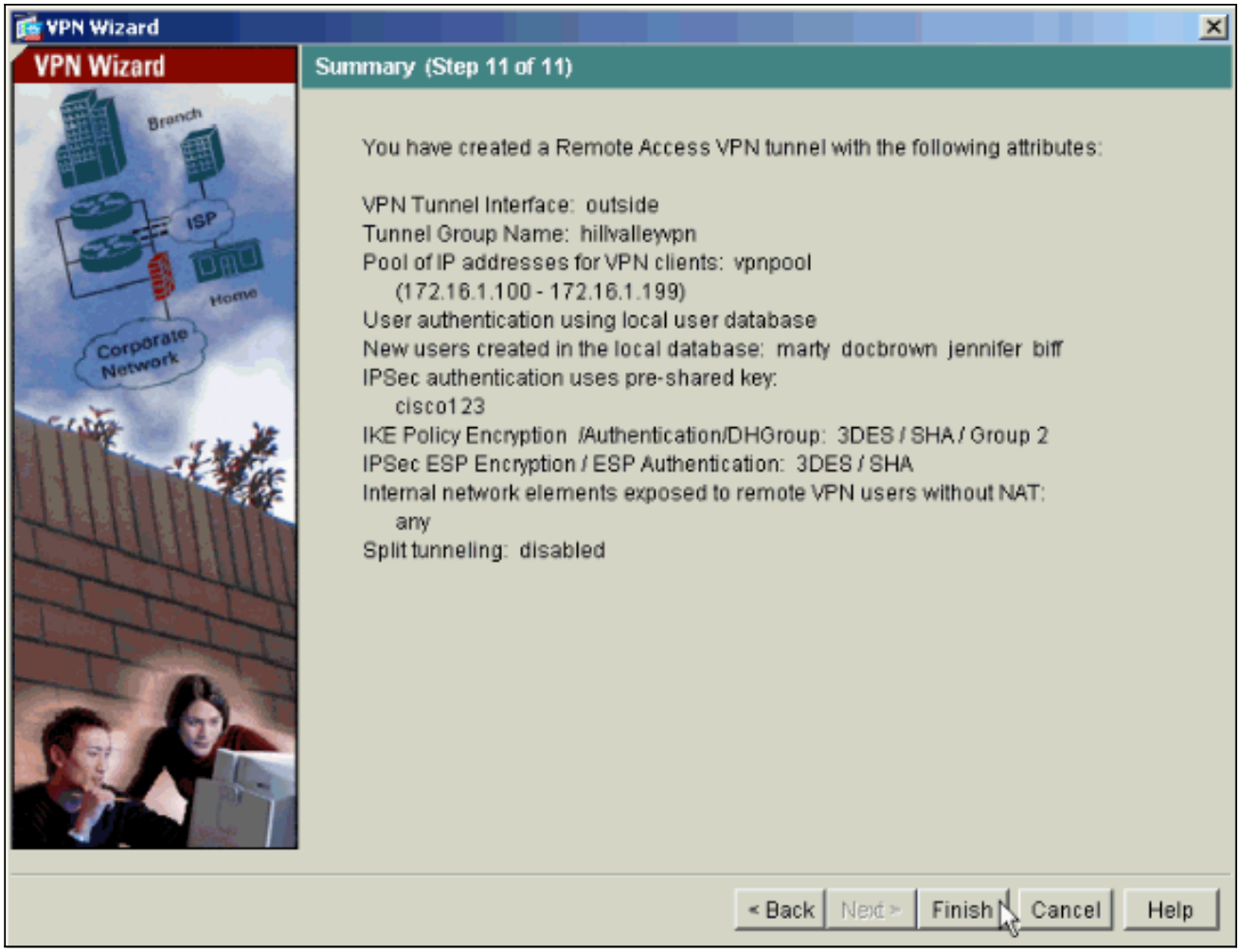
10. Specificeer de parameters voor IPSec, ook bekend als IKE fase 2.De configuraties aan beide zijden van de tunnel moeten precies overeenkomen. Maar de Cisco VPN-client selecteert automatisch de juiste configuratie voor zichzelf. Daarom is geen IKE-configuratie nodig op de client-
pc.



11. Specificeer welke, als om het even welke, interne hosts of netwerken zouden moeten worden blootgesteld aan externe VPN-gebruikers.Als u deze lijst leeg laat, staat het externe VPN-gebruikers toe om toegang te krijgen tot het gehele binnennetwerk van de ASA.U kunt ook gesplitste tunneling in dit venster inschakelen. Split-tunneling versleutelt het verkeer naar de bronnen die eerder in deze procedure zijn gedefinieerd en geeft onversleutelde toegang tot internet in het algemeen door dat verkeer niet uit te schakelen. Als gesplitste tunneling *niet* ingeschakeld is, wordt al het verkeer van externe VPN-gebruikers naar de ASA gekanaliseerd. Dit kan zeer bandbreedte en processor intensief worden, gebaseerd op uw
configuratie.



12. Dit venster geeft een samenvatting van de maatregelen die u hebt genomen. Klik op **Voltooien** als u tevreden bent met de configuratie.



ASA/PIX configureren als externe VPN-server met CLI

Voltooi deze stappen om een externe VPN-toegangsserver te configureren vanuit de opdrachtregel. Raadpleeg Beelden voor externe toegang VPN's of Cisco ASA 5500 Series adaptieve security applicaties-commando-referenties voor meer informatie over elke opdracht die wordt gebruikt.

1. Voer het **ip lokale pool** opdracht in in de mondiale configuratiemodus om IP adrespools te configureren om te gebruiken voor VPN-tunnels in de externe toegang. Voer de geen vorm van deze opdracht in om adrepools te verwijderen.Het beveiligingsapparaat gebruikt adrestoestellen op basis van de tunnelgroep voor de aansluiting. Als u meer dan één adrespool voor een tunnelgroep vormt, gebruikt het security apparaat deze in de volgorde waarin ze zijn geconfigureerd. Geef deze opdracht uit om een pool van lokale adressen te maken die kan worden gebruikt om dynamische adressen toe te wijzen aan VPN-clients met externe toegang:
```
ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
  255.255.255.0
```

2. Deze opdracht geven:
```
ASA-AIP-CLI(config)#username marty password 12345678
```

3. Geef deze reeks opdrachten uit om de specifieke tunnel te configureren:ASA-AIP-CLI (configuratie)**#isakmp beleid 1 verificatie vooraf delen**ASA-AIP-CLI (Config)**#isakmp beleid 1-encryptie 3des**ASA-AIP-CLI (configuratie)**#isakmp beleid 1 hashsha**ASA-AIP-CLI (configuratie)**#isakmp beleid 1 groep 2**ASA-AIP-CLI (configuratie)**#isakmp beleid 1 leven**

43200ASA 5500-AIP-CLI (configuratie)**#isakmp maakt toegang tot buiten mogelijk**ASA 5500-AIP-CLI (**configuratie**)**#crypto ipsec transformatie-set ESP-3DES-SHA esp-3des esp-sha-hmac**ASA-AIP-CLI (**configuratie**)**#crypto dynamisch-kaart buiten_dyn_map 10 set transformatie-set ESP-3DES-SHA**ASA-AIP-CLI (**configuratie**)**#crypto dynamisch-kaart buiten_dyn_map 10 set reverse-route**ASA-AIP-CLI (configuratie)**#crypto dynamisch-kaart buiten_dyn_map 10 ingestelde security-associatie levensduur seconden 288000**ASA-AIP-CLI (configuratie)**#crypto kaart buiten_map 10 ipsec-isakmp dynamisch buiten_dyn_map**ASA-AIP-CLI (configuratie)**#crypto kaart buiten_map interface**ASA 5500-AIP-CLI (**configuratie**)**#crypto nucleaire traversal**

4. *Optioneel:* Als u wilt dat de verbinding de toegangslijst overschrijdt die op de interface wordt toegepast, geeft u deze opdracht uit:
   ASA-AIP-CLI(config)#**sysopt connection permit-ipsec**

   Opmerking: deze opdracht werkt vóór 7.2(2) op 7.x-afbeeldingen. Als u afbeelding 7.2(2) gebruikt, geeft u de `ASA-AIP-CLI (configuratie)#sysopt verbinding vergunning-vpn` opdracht uit.
5. Deze opdracht geven:
   ASA-AIP-CLI(config)#**group-policy hillvalleyvpn internal**

6. Geef deze opdrachten uit om de instellingen voor de clientverbinding te configureren:ASA-AIP-CLI (configuratie)**#group-policy** hillvalleyvpn**-eigenschappen**ASA-AIP-CLI (configuratie)# (configuratie-groep-beleid)**#dns-server waarde 172.16.1.11**ASA 5500-AIP-CLI (configuratie)# (configuratie-groep-beleid)**#vpn-tunnel-protocol IPSec**ASA-AIP-CLI (configuratie)# (configuratie-groep-beleid)**#default-domeinwaarde test.com**
7. Deze opdracht geven:
   ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-ra**

8. Deze opdracht geven:
   ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-attributes**

9. Deze opdracht geven:
   ASA-AIP-CLI(config-tunnel-ipsec)#**pre-shared-key cisco123**

10. Deze opdracht geven:
    ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn general-attributes**

11. Geef deze opdracht uit om de lokale gebruikersdatabase voor authenticatie te raadplegen.
    ASA-AIP-CLI(config-tunnel-general)#**authentication-server-group LOCAL**

12. Associeer het groepsbeleid met de tunnelgroep
    ASA-AIP-CLI(config-tunnel-ipsec)# **default-group-policy hillvalleyvpn**

13. Geef deze opdracht uit in de algemene-attributenmodus van de hillvalleyvpn-tunnelgroep om de vpnpool die in stap 1 is gemaakt, aan de hillvalleyvpn-groep toe te wijzen.
    ASA-AIP-CLI(config-tunnel-general)#**address-pool vpnpool**

Config op het ASA-apparaat uitvoeren
ASA-AIP-CLI(config)#**show running-config** ASA Version 7.2(2) ! hostname ASAwAIP-CLI

```
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp.com
pager lines 24
mtu outside 1500
mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy hillvalleyvpn1 internal
group-policy hillvalleyvpn1 attributes
 dns-server value 172.16.1.11
 vpn-tunnel-protocol IPSec
 default-domain value test.com
username marty password 6XmYwQOO9tiYnUDN encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
```

```
sha-hmac
crypto dynamic-map outside_dyn_map 10 set transform-set
ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 10 set security-
association lifetime seconds 288000
crypto map outside_map 10 ipsec-isakmp dynamic
outside_dyn_map
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal  20
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
 address-pool vpnpool
 default-group-policy hillvalleyvpn
tunnel-group hillvalleyvpn ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192
: end
ASA-AIP-CLI(config)#
```

Configuratie van Cisco VPN-clientwachtwoord

Als u meerdere Cisco VPN-clients hebt, is het heel moeilijk om alle VPN-clientnamen en -wachtwoorden te onthouden. Om de wachtwoorden in de VPN-clientmachine op te slaan, moet u de ASA/PIX- en de VPN-client configureren zoals in dit gedeelte wordt beschreven.

ASA/PIX

Gebruik de opdracht **groepsbeleid eigenschappen** in mondiale configuratiemodus:

```
group-policy VPNusers attributes
  password-storage enable
```

Cisco VPN-client

Bewerk het **.pcf-bestand** en wijzig deze parameters:

```
SaveUserPassword=1
UserPassword=
```

Uitgebreide verificatie uitschakelen

In tunnelgroepsmodus, voer deze opdracht in om de uitgebreide authenticatie uit te schakelen, die standaard ingeschakeld is op PIX/ASA 7.x:

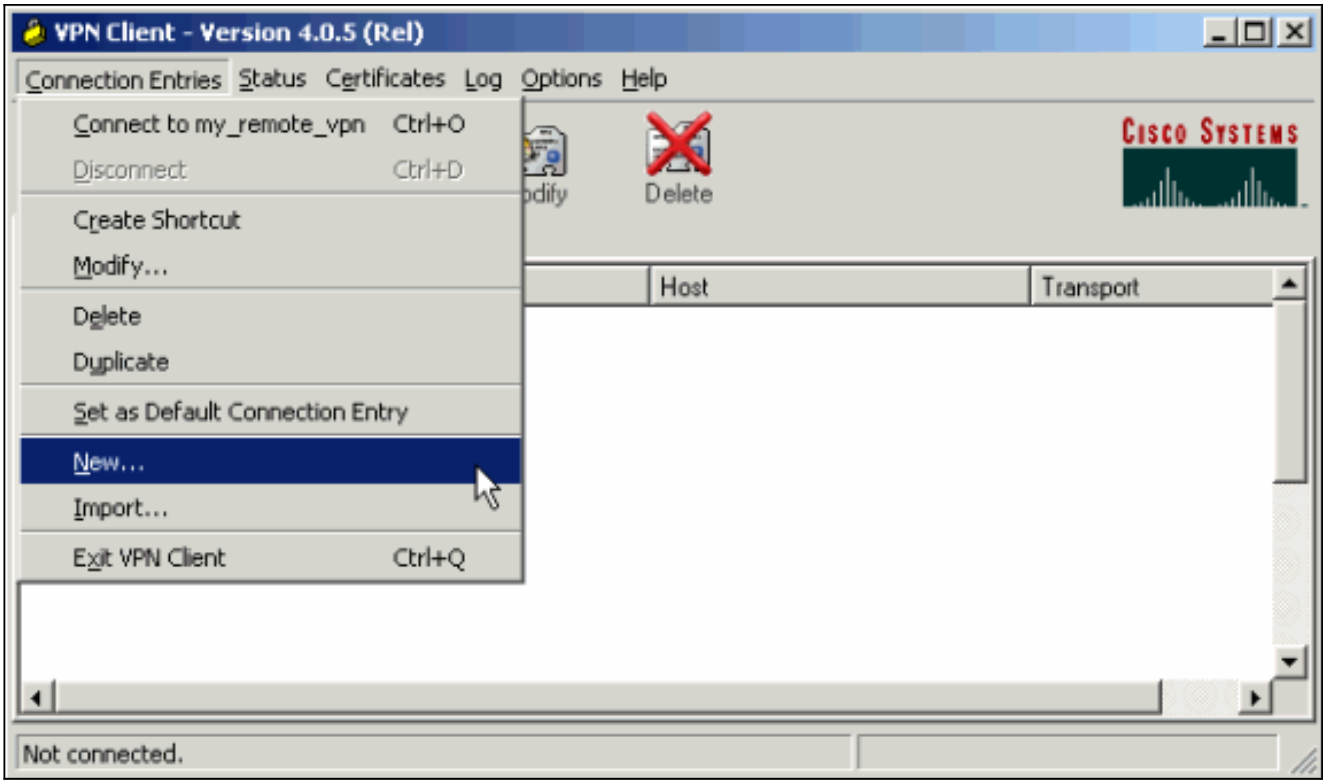
```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

Nadat u de uitgebreide authenticatie uitschakelt, zetten de VPN-clients geen gebruikersnaam/wachtwoord voor een verificatie (Xauth) op. Daarom heeft de ASA/PIX niet de gebruikersnaam en de wachtwoordconfiguratie nodig om de VPN-clients te authenticeren.

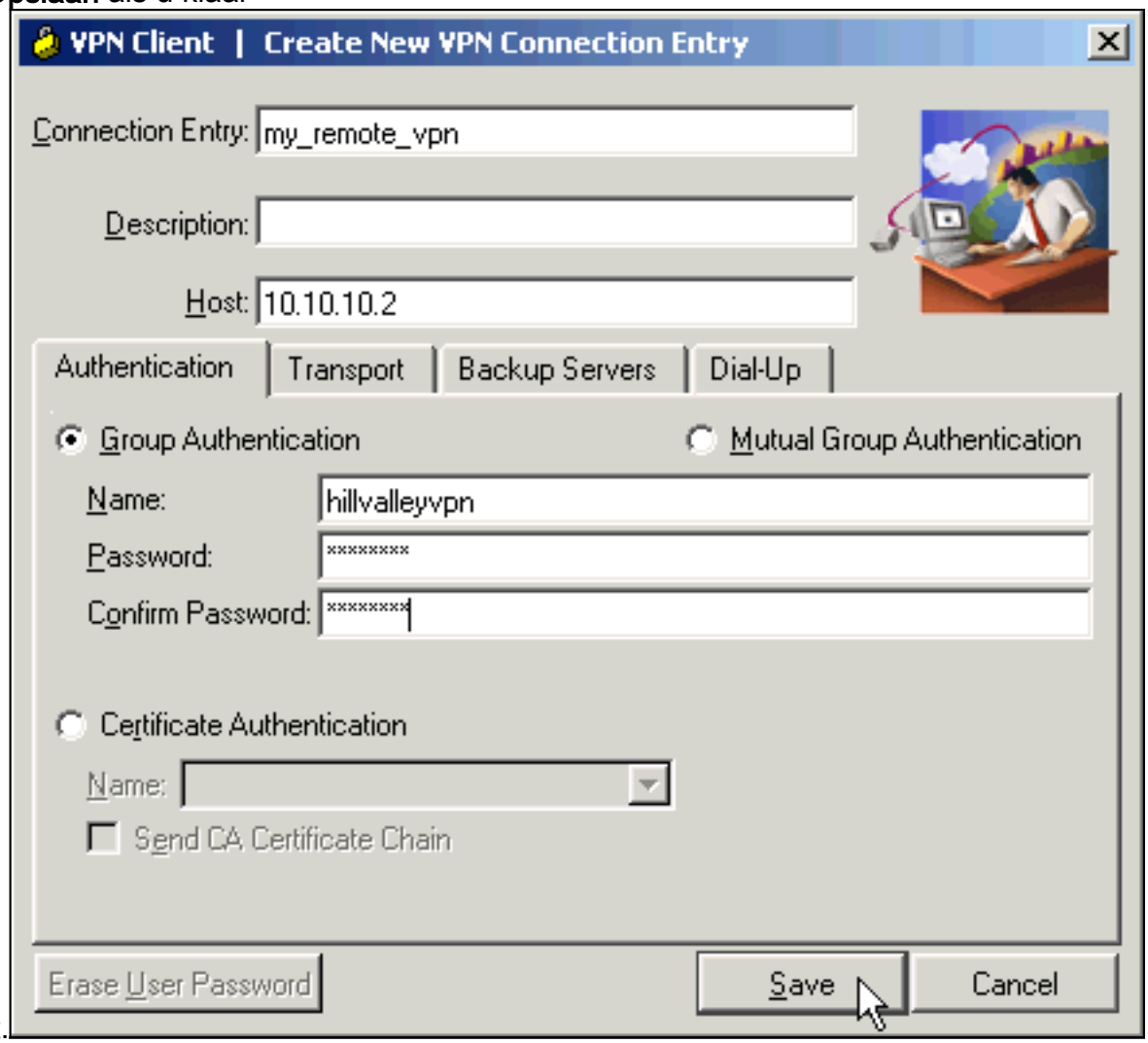
Verifiëren

Probeer met de Cisco ASA te verbinden aan het gebruik van de Cisco VPN-client om te controleren of de ASA met succes is geconfigureerd.

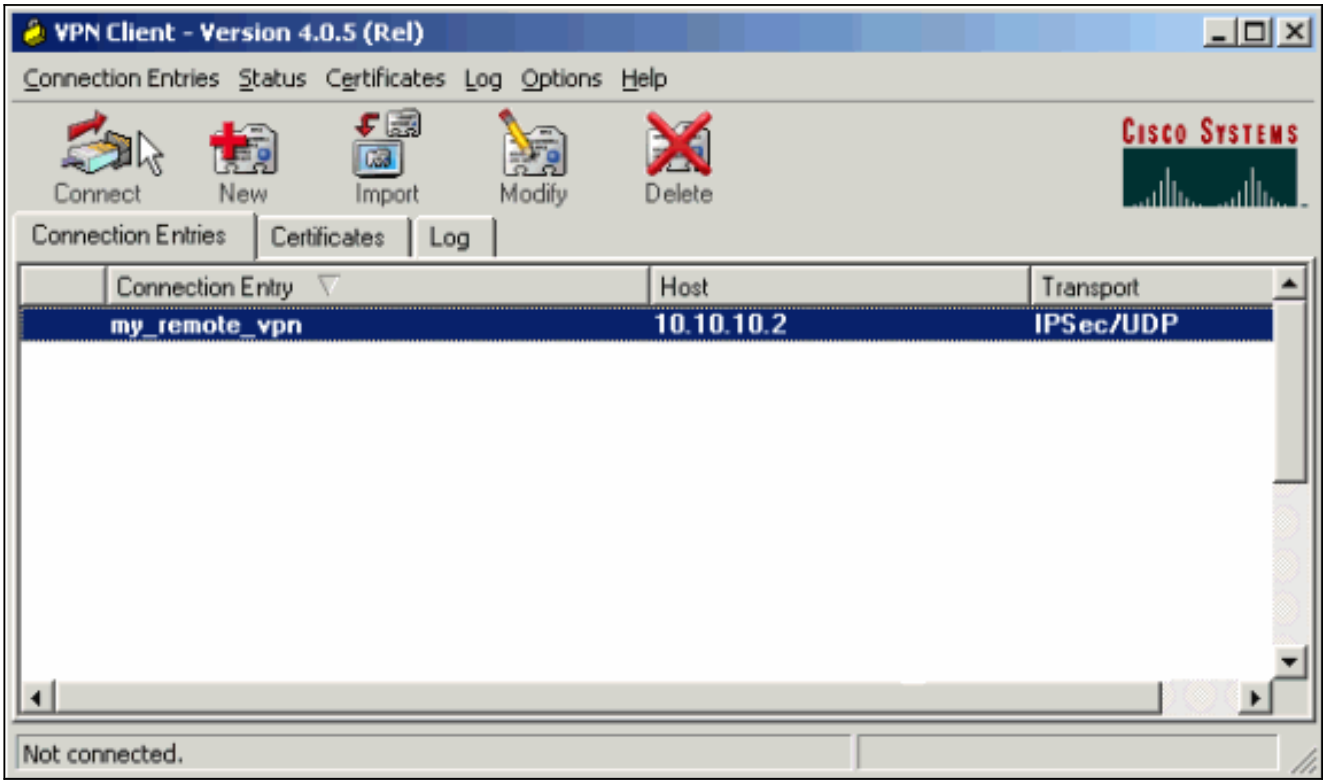
1. Selecteer **Connection Vermeldingen > New**.



2. Vul de gegevens in van uw nieuwe aansluiting.Het veld Host moet het IP-adres of de hostnaam van de eerder geconfigureerd Cisco ASA bevatten. De informatie over de groepsverificatie dient overeen te komen met de informatie die in stap 4 wordt gebruikt. Klik op **Opslaan** als u klaar bent.

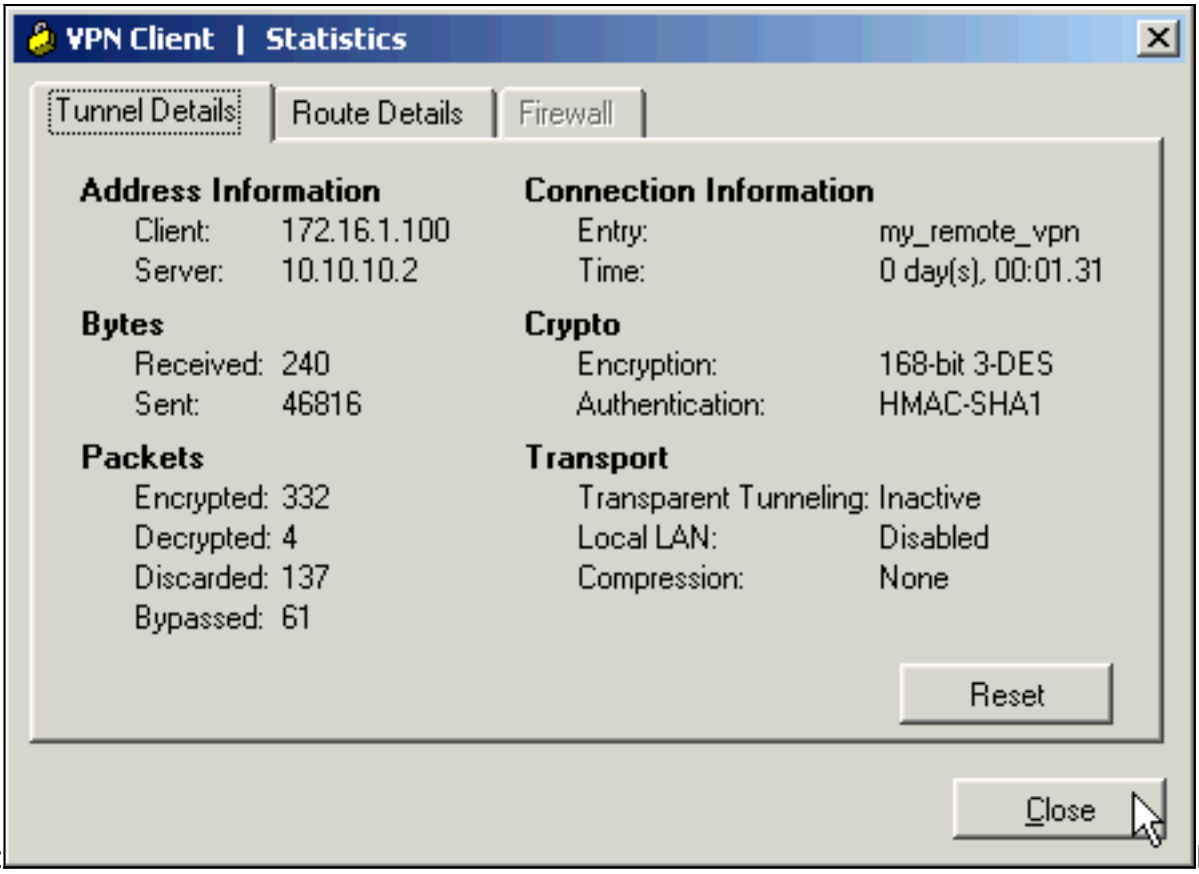


3. Selecteer de nieuwe verbinding en klik op **Connect**.

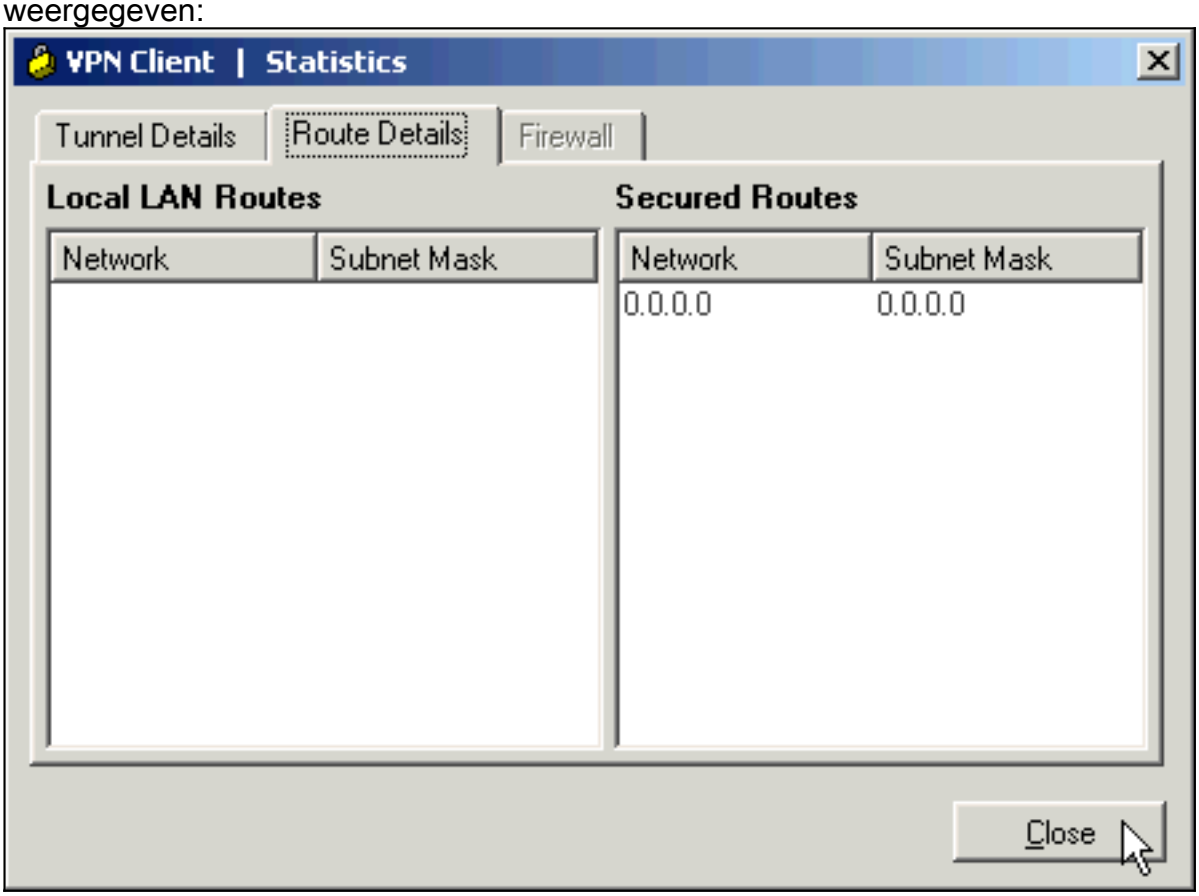


4. Voer een gebruikersnaam en wachtwoord in voor uitgebreide verificatie. Deze informatie moet overeenkomen met de informatie die in stap 5 en 6 is gespecificeerd.

5. Zodra de verbinding met succes is ingesteld selecteert u **Statistieken** uit het menu Status om de details van de tunnel te controleren.Dit venster toont informatie over verkeer en



crypto:In dit venster wordt informatie over gesplitste tunneling weergegeven:



Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Onjuiste encryptie-ACL

ASDM 5.0(2) is bekend om een crypto toegangscontrolelijst (ACL) te maken en toe te passen die problemen kan veroorzaken voor VPN-clients die gesplitste tunneling gebruiken, evenals voor hardwareclients in netwerk-extensiemodus. Gebruik ASDM versie 5.0(4.3) of hoger om dit probleem te voorkomen. Raadpleeg Cisco bug-ID CSCsc10806 (alleen geregistreerde klanten) voor meer informatie.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- Populairste oplossingen voor IPsec gemeenschappelijk L2L en Remote Access IPsec VPN-probleemoplossing
- Cisco ASA 5500 Series adaptieve security applicaties, probleemoplossing en meldingen
- Technische ondersteuning en documentatie – Cisco Systems